Security Aware Virtual Base Station Placement in 5G Cloud Radio Access Networks

Tshiamo Sigwele[1], Prashant Pillai[2] and Yim-Fun Hu[1]

[1] Faculty of Engineering and Informatics, University of Bradford, Bradford, West Yorkshire,BD7 1DP, UK
{T.Sigwele,Y.F.Hu}@bradford.ac.uk,
[2] Faculty of Technology, Design and Environment, Oxford Brookes University, Oxford, UK,
ppillai@brookes.ac.uk

Abstract. In fifth generation (5G) cloud radio access networks (C-RAN), baseband processing of base stations (BS's) will be processed on virtual machines called virtual BSs (VBS) in the centralized cloud architecture. The existing researches mostly focus on how to maximize resource utilization and reduce energy consumption in 5G C-RAN using VBS placement. However, security issues in the context of VBS placement within 5G C-RAN have been rarely addressed. In this paper, a security aware VBS placement (SAV) scheme within 5G C-RAN is proposed where the placement of VBSs to physical machines (PMs) considers the security levels of both the VBS and the PM. A rigorous simulation study is conducted for validating the proposed scheme, which shows a significant security improvement 16% compared to the heuristic simulated scheme (HSA).

Key words: 5G, cloud computing, C-RAN, cloud security, virtual machine placement.

1 Introduction

The fifth generation (5G) cellular networks will experience a thousand-fold increase in data traffic with over 100 billion connected devices by 2020 [1]. Such surge in traffic will be from smart-phones, tablets, machine-machine connections and the Internet of Things (IoT). In order to support this sky-rocketing traffic demand, heterogeneous cloud radio access H-CRAN networks has been proposed where macro remote radio heads (RRHs) are overlaid by smaller cell RRHs like femto, pico, micro and relay to increase capacity using spatial frequency reuse. The 5G C-RAN uses cloud computing virtualization techniques to host BS function in virtual machines (VMs) called virtual basestation (BSs) (VBSs) in the BS cloud [2]. One of the driving forces in the BS cloud is VBS placement where VBS are migrated among physical machines (PMs) to maximise BS resource utilization and reduce energy consumption. Nevertheless, security issues in the BS cloud in C-RAN have been rarely addressed. The introduction of running BS functions in PMs in the BS cloud brings about security issues.

A prevalent VBS image with known vulnerabilities can be instantiated by an attacker in BS cloud, therefore it may generate a large number of security holes for attackers which may include eavesdropping users conversation. The introduction of VBS images with known security vulnerabilities to a PM can lead to security risks to the co-located VBSs in that PM. This is because of the one to many mapping between the PM and the VBSs which makes vulnerabilities propagate rapidly across the entire BS cloud. Some of the attacks that an attacker can introduce include compromising the hypervisor and also side channel attacks to the VBSs co-located within the same PM [3]. A VBS that has been compromised can infect other VBS sharing the same hypervisor, memory or CPU. When a VBS with no security risks is migrated to the PM with a compromised VBS, that VBS will be compromised too. As such there is need for a security aware VBS placement in the BS cloud to avoid the security risks.

In this paper, a VBS and PM security evaluation based on their vulnerabilities is first conducted then, based on these security evaluations, a novel security aware VSB placement is developed which minimises the security risks in the BS cloud. The VBSs and PMs are grouped into vulnerability levels such that a VBS with low vulnerability will be allocated to a PM with low vulnerability and a VBS with high vulnerability will be allocated to a PM with high vulnerability. The rest of the paper is organised as follows. Section 2 describes the related work on VBS placement in C-RAN. The proposed security aware VBS placement framework is described in details in Section 3. The results and discussions are presented in Section 4. Then Finally the conclusions are presented in Section 5.

2 Related Work

Researchers have proposed several VBS placement strategies to improve resouce utilization and improve energy consumption within 5G C-RAN. However, to the best of our knowledge, there are no efforts on VBS placement strategies in 5G C-RAN to minimize the security risks for the BS cloud platform. The author in [4] proposed a VBSs virtualization scheme that minimizes the power consumption with a linear computational complexity order. The scheme is based on a heuristic simulated annealing (HSA) algorithm, which combines a bin packing algorithm with simulated annealing. Simulation results show that the HSA effectively decreases system power consumption when compared to standard approaches. However, the simulated annealing VBS placement scheme does not consider security in migration of VBSs. Authors in [5] proposed a BBU reduction scheme for C-RAN that allocates VBSs to RRHs based on the imbalance of subscribers in office/residential areas. A set of upper limit of VBS utilization is defined to avoid overloading of the VBS. However, the author did not consider security in their VBS consolidation scheme. S. Namba et al. in [6] proposed a baseband unit (BBU) reduction network architecture called Colony-RAN due to its ability to flexibly change cell layout by changing the connections of BBUs and RRHs in respect to traffic demand. However, the

proposed method has frequent ping pong reselections of RRH to BBU. The author in [7] proposed a model for reducing power consumption in H-CRAN by turning off the BBU in the cloud. However, the author assumes that all the BBUs in the BS cloud operate at full load which is unrealistics. The author in [8] proposed a VBS virtualization scheme that minimizes the power consumption of the BS cloud. The VBS virtualization problem is formulated as a bin packing problem, where each VBS is treated as a bin with finite computing expressed in million Operations per Time Slot (MOPTS). The dynamics of the cell traffic load is treated as an item that needs to be packed into the bins with the size equal to the computing resources in MOPTS, required to support the traffic load. Nevertheless, security has not been considered. Authors in [9] proposed a C-RAN system using virtualization technology on general purpose processors (GPPs) where BBUs are dynamically provisioned according to traffic load. In [10], L. Cheng et al. developed an energy efficient C-RAN system with a reconfigurable backhaul that allows 4 BBUs to connect flexibly with 4 RRHs using radio-over-fiber technology. The backhaul architecture allows the mapping between BBUs and RRHs to be flexible and changed dynamically to reduce energy consumption in the BBU pool. However, the paper assumes static user traffic whereas in reality BS traffic is dynamic.

3 Proposed Security Aware VBS Placement (SAV)

3.1 System Model

The proposed architecture of SAV is shown in Fig. 1. The system comprise of 5G heterogeneous network which is made up of macro RRH overlaid by femto, pico, micro and relay RRHs. The RRHs from the radio side are connected to the BS cloud via high speed, low latency fiber cables. These connection is called the fronthaul [2]. The fronthaul in the BS cloud is first connected to the dispatcher which route data to their respective VBSs within physical machines (PMs) according to some VBS placement rules from the SAV module in the controller. The SAV module in the controller contains the VBS placement framework which will be explained in details in Section 3.3. The SAV takes all VBSs and PMs as inputs and output the VSB-PM map. The BS cloud also comprise of the PMs which host VBSs. The PMs contains hypervisors which runs on top of the PM operating system (OS). The hypervisor is responsible for creating VBS on the PMs. Each RRH has its own VBS.

3.2 VBS and PM Security Evaluation

The security evaluation procedure consists of evaluating the risks of both the VBSs and PMs in the BS cloud.

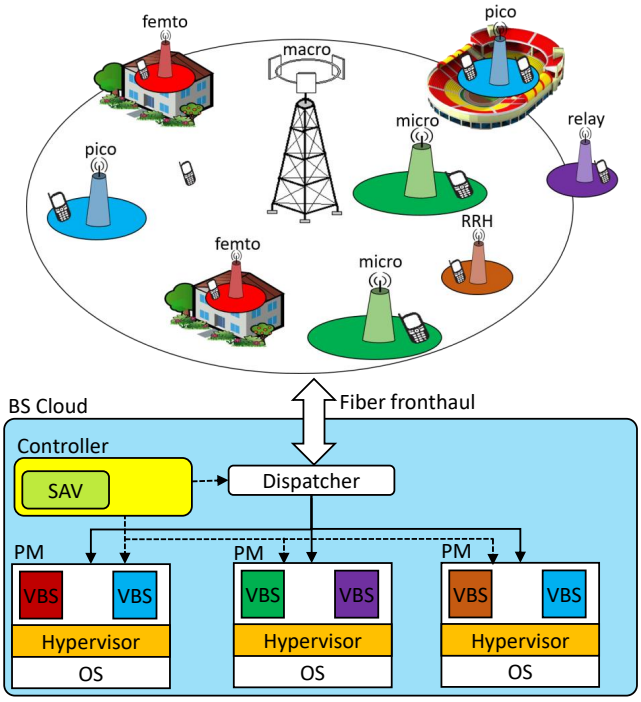

Fig. 1. The proposed SAV architecture.

VBS Security Evaluation: First, we quantify each VBS's vulnerabilities based on the US National Vulnerability Database (NVD) [11], in which all vulnerabilities called common vulnerability and exposures (CVE) are scored according to the Common Vulnerability Scoring System (CVSS) [3]. The NVD is the repository which provides CVSS scores for all CVE vulnerabilities. At present, NVD contains information about over 69,000 CVE vulnerabilities (as of 04/27/2015) [3]. NVD was created by the government of United States to help the Department of Homeland Security to warn public about common computer vulnerabilities. These vulnerabilities now include latest attacks on cloud computing environments. The CVSS base score is the primary metric and describes the severity of the vulnerability. The base score uses an interval scale of (0, 10) to measure the severity of vulnerabilities.

First a check is perfomed with NVD to collect potential vulnerabilities in the VBSs. Vulnerability scanner tools, such as, Nessus and Qualys are available to conduct this job. Since it is possible for a VBS to have more than one vulnerabilities, it is usually desirable to aggregate the scores of individual vulnerabilities for each VBS. The VBS vulnerability can be divided into three descrete levels: low compromise, medium compromise and high compromise. Suppose the collected vulnerabilities of all the VBSs within PM_i are stored

in the set $V_{PM_i} = \{V_j | j = 1, 2, ...n\}$. Then the compromise level of a VBS_j denoted C_{VBS_j} can be given as:

$$C_{VBS_j} = \frac{V_j}{\sum_{m=1}^{n} V_m} \tag{1}$$

Physical Machine Security Evaluation: The VBS compromise level has been computed. Next the probability of survivability for each PM is computed based on the compromise level (C_{VBS_j}) of each hosted VBS. The survivability probability is the possibility that all owned VBSs of a PM can survive during the attacks in one or more of the VBSs. If any of the VBSs in the PM is compromised, then the PM will also be compromised with high probability. Given the compromise level of all VBSs in PM_i as $\{C_{VBS_1}, C_{VBS_2}, ..., C_{VBS_n}\}$, then the survivability score for PM_i denoted as S_{PM_i} is given as:

$$S_{PM_i} = \prod_{m=1}^{n} (1 - C_{VBS_j}) \tag{2}$$

The survivability quantifies the PM security level which correspond to three discrete states: low survivability, medium survivability and high survivability. Next the VBS placement based on the VBS and PM security levels is described in the next section.

3.3 The SAV Framework

From the previous discussions, we can learn that the success of attacks highly depends on the placement strategy of the cloud. Thus, our approach is to find a systematic solution to place VBSs into PMs which can reduce security risks in the BS cloud. If a VBS has low compromise, it will be infeasible to place it on a PM with low survivability. Also, if a PM is of high survivability, it would be infeasible to place a VBSs with high compromise which may results in a negative survivability impacts on the PM. In the proposed SAV scheme, the compromise level of the VBS and the survivability of the PM are taken into consideration when performing VBS placement. In SAV, it will be reasonable to place a VBS of low compromise level to a PM with high survivability. Also, in SAV, the VBSs are placed to PMs such that the C_{VBS_j} state match the S_{PM_i} state as follows:

i) A low compromise VBS is placed on high survivability PM
ii) A medium compromise VBS is placed on medium survivability PM
iii) A high compromise VBS is placed on low survivability PM

Fig. 2 shows the flowchart of how the proposed SAV scheme operate. The input to the SAV scheme is all the VBSs and all the PMs in the BS cloud. First for every VBS, the security evaluation is performed by computing the comprise level of each VBS using equation (1). Then the compromise level (C_{VBS_j}) is used for calculating survivability of each PM (S_{PM_i}). A test is then performed on each VBS to check whether the compromise state of that VBS match the survivability

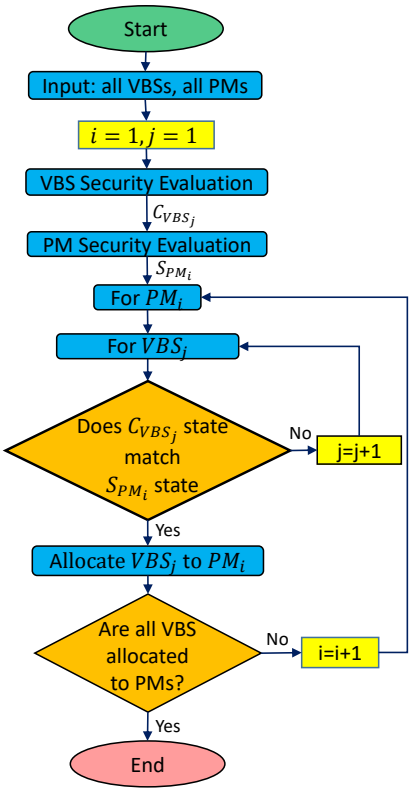

Fig. 2. The flowchart of SAV framework.

of the PM. If not, then all the other VBS compromise levels are checked and if they match the PM survavibility state, the VBS is then allocated to the PM. The process will continue untill all VBSs are allocated to PMs securely.

4 Results and Discussion

To analyse the proposed SAV framework, a 2 tier H-CRAN long term evolution (LTE) layout is considered where macro RRHs are overlaid by small cells RRHs. Up to 200 RRHs are considered and each RRH has its own VBS in the BS cloud. As explained before, to the best of our knowledge, there are no security aware VBS placement schemes in 5G C-RAN at the moment, this paper is the first to proposed such framework. Therefore, the proposed SAV will be compared with the HSA scheme in [4] which consider VBS placement for saving energy consumption in the BS cloud without considering security. Fig. 3 shows the effects of increasing the number of VBSs in the network on the PM survivability for all the schemes. For both the proposed SAV scheme and the HSA schemes,

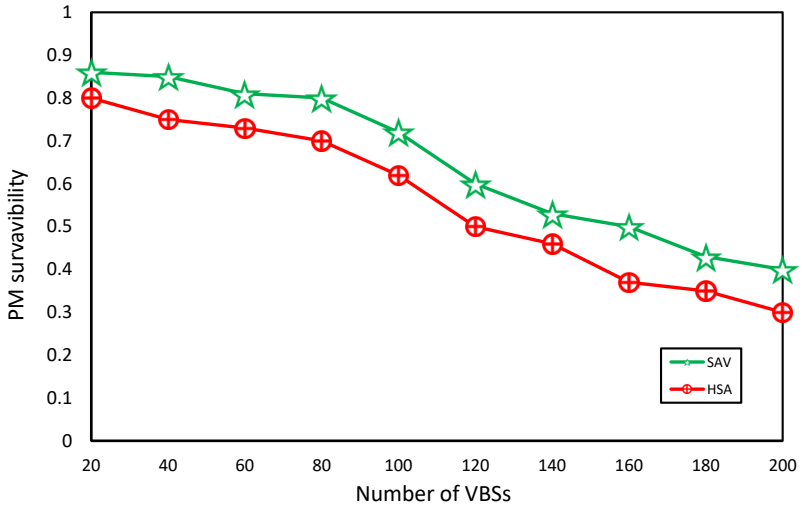

Fig. 3. The effects of VBS variation on PM survivability.

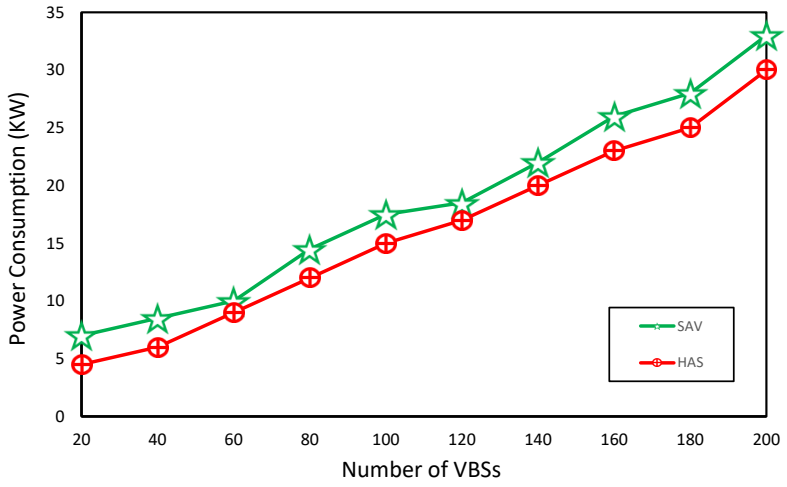

Fig. 4. The effects of VBS variation on power consumption.

as the number of VBSs in the BS cloud increases, the PM survivability decreases because the chances of comprimised VBSs are higher with the increase of VBSs. Also it can be observed in the diagram than the SAV scheme performs better than the HSA scheme by 16% with high chances of survivability of an average of 0.65 compared to the HSA scheme with chances of survivability of 0.5. This is because the SAV scheme considers security of VBSs and PMs before performing the VBS placement. Fig. 4 shows the effects of varying the number of VBSs on the power consumption in the BS cloud. For both the schemes, as the number of VBSs

increases, the power consumption also increases as more VBSs requires more PMs which will consume more power. On average, the SAV scheme consumes 15% more energy compared to the HSA scheme. This is because, even though the SAV scheme provide some security benefits, this results in the penalty of more power of 15% being consumed by the SAV scheme as a results of the VBS placement scheme security overheads which requires more PMs to be deployed.

5 Conclusion

The existing researches mostly focus on how to maximize resource utilization and reduce energy consumption in fifth generation (5G) cloud radio access networks (C-RAN) using virtual base station (VBS) placement. However, security issues in the context of VBS placement within 5G C-RAN have been rarely addressed. In this paper, a security aware VBS placement (SAV) scheme is proposed where the placement of VBSs to physical machines (PMs) considers the security levels of both the VBS and the PM. A rigorous simulation study is conducted for validating the proposed scheme, which shows a significant security improvement since the proposed SAV scheme outperforms the heuristic simulated scheme (HSA) by 16% with power consumption penalty of 15%.

References

1. 5G: A Technology Vision,Huawei Tech. White Paper, 2013
2. Chen, K., Duan, K.:C-ran:The road towards green ran. In:China Mobile Research Institute white Paper, 2011.
3. Yuchi, X., Sachin, S.:Enabling security-aware virtual machine placement in IaaS clouds. In:Military Communications Conference, MILCOM 2015-2015 IEEE. pp. 1554–1559(2015).
4. Qian, M., Hardjawana, W., Shi, J., Vucetic, B.:Baseband processing units virtualization for cloud radio access networks. In:IEEE Wireless Communications Letters. vol 4, pp. 189–192. IEEE (2015).
5. Namba, S., Warabino, T., Kaneko, K.:Bbu-rrh switching schemes for centralized ran. In:2012 7th International ICST Conference on Communications and Networking in China (CHINACOM). IEEE.pp. 762–766(2012).
6. Namba, S., Matsunaka, T., Warabino, T.:Colony-ran architecture for future cellular network. In:Network & Mobile Summit (FutureNetw). IEEE.pp. 1–8(2012).
7. Domenico, A., Katranaras, E.:Energy efficiency benefits of RAN-as-a-service concept for a cloud-based 5G mobile network infrastructure. In:IEEE Access. vol 2, pp. 1586–1597(2014).
8. Qian, M., Hardjawana, W, Vucetic, B.:Baseband processing units virtualization for cloud radio access networks. In:IEEE Wireless Communications Letters. vol 4, no. 2, pp. 189–192(2015).
9. Kong, Z., Gong, C., Xu, Z.:ebase: A baseband unit cluster testbed to improve energy-efficiency for cloud radio access network. In:IEEE International Conference on Communications (ICC). IEEE.pp. 4222–4227(2013).

10. Liu, C., Sundaresan, K., Jiang, M., Rangarajan, S., & Chang, G. K.:The case for re-configurable backhaul in cloud-RAN based small cell networks. In:IEEE INFOCOM, 2013 Proceedings. IEEE, pp. 1124–1132(2013).
11. United State Government.:US National Vulnerability Database,https://nvd.nist.gov[Accessed:March 2017]